Journal of Computer and Knowledge Engineering, Vol. 9, No. 1, 2026. (37-58)

Ferdowsi University of Mashhad

Journal of Computer and Knowledge Engineering

https://cke.um.ac.ir

Information and Communication Technology Association of Iran

Spectrum Anomaly Detection: A Deep Learning Approach*

Research Article

Motahareh Aghalari[1], Hossein Khaleghi bizaki[2]

10.22067/cke.2025.91456.1144

Abstract *The frequency spectrum is a limited and valuable resource and faces challenges due to anomalies. Hence, the detection of anomalies in the frequency spectrum is crucial for maintaining the integrity and reliability of telecommunication systems. These anomalies, which include jamming signals and interference, can disrupt communication channels and degrade system performance. This paper presents a comprehensive review of deep learning applications in spectrum anomaly detection, focusing on research conducted between 2017 and 2024. The review examines various pre-processing techniques used in spectrum anomaly detection, highlighting the widespread use of spectrogram and short-time Fourier transform (STFT), particularly in reconstruction-based methods, due to their effectiveness in capturing time-frequency information despite their computational challenges. Additionally, the study underscores the importance of selecting appropriate problem-solving approaches, such as classification, segmentation, or object detection, and tailoring models to suit specific tasks. These findings underscore the potential of deep learning-based approaches in enhancing spectrum monitoring and interference management.*

Key Words Anomaly, Deep learning, Interference, Spectrum.

1. Introduction and Related Work

The frequency spectrum, a limited and valuable resource, serves as the backbone for wireless communication networks [1, 2]. However, its optimal utilization faces challenges due to anomalies that may arise from interference, equipment malfunction, unauthorized access, or other unexpected events. Detecting these anomalies is vital for maintaining network performance, avoiding disruptions, and ensuring compliance with regulatory standards. In general, any factor that causes a change in the behavioral pattern of data is recognized as an anomaly. This can include unexpected events resulting from behavior that deviates from the user's perspective, isolated incidents, or the presence of disruptive elements within the system [3]. Unusual events that deviate from common patterns are often recognized as anomalies. For instance, a sudden gathering of people in a specific area or motorcyclists appearing on sidewalks are considered abnormal behaviors [4-6]. An unwanted, isolated occurrence within a dataset is also classified as an anomaly; for instance, a sudden, one-time change in the intensity of received signals [7-9]. Similarly, in the medical field, phenomena such as tumors, which threaten an individual's health, are considered anomalies [10, 11]. The presence of jamming signals that disrupt communication is another example of an anomaly in telecommunications.

This paper focuses specifically on anomaly detection in the radio frequency (RF) spectrum, where disruptions such as interference or jamming can significantly impact communication reliability and spectrum efficiency. The occurrence of anomalies leads to changes in the behavioral pattern of the spectrum. The frequency spectrum usually exhibits a specific behavior when telecommunication signals are present. If an unknown phenomenon or anomaly occurs, this regular behavior is altered. Therefore, by learning the behavioral pattern of the spectrum, the occurrence of anomalies can be identified [12, 13].

Advances in computational systems and access to large datasets have enabled the use of artificial intelligence (AI) tools[14]. These tools analyze data and accurately detect anomalies. Time-series anomaly detection is applied in various fields, such as urban management, intrusion

* Manuscript received January 01, 2025, Revised May 30, 2025, Accepted October 04, 2025.

[1] Ph.D. Student, Computer and Electrical Engineering Department, Malek-Ashtar University of Technology, Tehran, Iran. **Email:** motahare.aghalari@gmail.com

[2] Corresponding author, Professor, Computer and Electrical Engineering Department, Malek-Ashtar University of Technology, Tehran, Iran. **Email:** bizaki@yahoo.com

detection, and medical diagnostics[15, 16]. Continuous observation during spectrum monitoring ensures prompt detection of anomalies and the implementation of appropriate actions.

In recent years, AI methods have emerged as the most widely used approach for anomaly detection. This interest in AI stems from its ability to deliver better performance, particularly in solving complex problems like detecting the time and frequency of spectrum anomalies, as well as faster inference after model training. AI-based algorithms enable the development of systems that can learn the behavior of a normal spectrum (without anomalies) and detect and classify various types of anomalies. Among AI methods widely used for spectrum monitoring, deep learning (DL) models have become the most prevalent in some studies [17-21]. These models, inspired by the structure of the human brain, can extract hierarchical patterns from data. In blind detection scenarios, where there is no prior knowledge about the signal, machine learning and deep learning tools become invaluable for uncovering inherent patterns within the data and enabling effective signal identification.

Given the extensive body of research in this area, numerous review articles have been published on spectrum anomalies, each offering a distinct analytical perspective. Table 1 summarizes and compares the most relevant works in this domain. However, a detailed examination of these studies reveals several critical limitations that our work directly addresses. Below, we outline these shortcomings and highlight our corresponding contributions:

- ***Mapping Conceptual Anomaly Types to Deep Learning Techniques***: We propose a novel conceptual classification of spectral anomalies into known and unknown categories. This distinction is essential, as it informs the selection of the most appropriate deep learning models based on the nature of the anomaly. Building on this framework, we establish a direct mapping between anomaly types and deep learning approaches, such as classification, reconstruction, detection, and segmentation, offering practical guidance for model selection. In contrast, previous surveys [22-25] primarily define anomalies based on application domains (e.g., jamming, interference) or signal sources (e.g., intentional vs. unintentional), without providing an explicit linkage between anomaly types and suitable deep learning techniques.
- ***Comparative Analysis of Pre-processing Techniques***: Existing studies [22, 23] mention pre-processing techniques only briefly and do not assess their impact on deep learning model performance. Other relevant surveys [24, 25] discuss certain methods but lack a systematic comparative evaluation or apply pre-processing solely as part of the model input without further analysis. This absence of a thorough comparison represents a significant research gap, which we address by providing a comprehensive evaluation of pre-processing techniques for spectral anomaly detection.

TABLE 1
Comparison of Related Surveys on Deep Learning for Spectrum Anomaly Detection

Aspect	**Pirayesh et al.** [22]	**Oyedare et al.** [24]	**Lohan et al.** [23]	**Lancho et al.** [25]	**Ours**
Year Published	2021	2022	2024	2025	2025
Main Focus	Jamming	Interference + Jamming	Interference + Jamming	RF signal separation (mixed sources)	Interference + Jamming
Anomaly Type	Protocol-level attack types	Signal-type anomalies	Intentional vs. unintentional	Mixed / unknown anomalies	Known vs. Unknown anomalies
Pre-processing Comparison	Brief mention	Brief mention	Brief comparison	Used in model inputs only	✓ Systematic comparative analysis
AI Model Comparison	✕Limited discussion	✓Systematic overview of DL models	✕Brief comparison	✓Benchmarked (UNet, WaveNet)	✓Deep model–approach-based comparison
DL Techniques vs. Anomaly Type	✕ Not addressed	✕ Not explicitly compared	✕ Not anomaly-specific	✕ Task-specific, not anomaly-specific	✓ Explicit mapping of DL methods to anomaly types
Unique Contribution	Protocol-level jamming taxonomy and mitigation strategies	Survey of DL-based interference suppression methods	Review of AI-based interference in 5G/6G systems	RF Challenge dataset + DL benchmarking	Novel anomaly taxonomy and methodological comparison of different models across deep learning approaches (classification, detection, object detection, and segmentation).

- ***AI Model Comparison – Scope and Depth of Review*:** We provide an updated review of deep learning-based spectrum anomaly detection methods, covering up to the year 2024. While the survey in [24] offers a structured overview of deep learning models, its coverage is limited to studies published before 2021. Additionally, prior works [22, 23] provide limited analysis and only a superficial review of AI methods, or focus exclusively on AI applications and introduce a benchmark dataset for next-generation networks [25].
- ***Challenges and Future Directions:*** In addition to the above, we discuss existing research gaps, including the challenges of detecting hybrid anomalies, generalizing models across varying conditions.

  The remainder of this paper presents background on spectrum anomaly detection, reviews deep learning methods and pre-processing techniques, compares existing approaches, and concludes with key insights and future directions.

2. BACKGROUND

A. Categorization of Spectrum Anomalies

In addition to the conventional anomaly categories noted in prior work [22-25], this review introduces the distinction between known and unknown anomalies, a perspective that, to our knowledge, has not yet been explicitly applied to spectrum anomaly detection.

Known anomalies: These anomalies refer to disruptions whose features (e.g., signal shape, power level, and duration) have been previously observed or modeled. Detection approaches for these anomalies typically rely on supervised learning techniques or signature-based methods that use labeled datasets.

Unknown anomalies: These are previously unseen or unpredictable events that do not appear in the training data, making them much harder to detect. Approaches targeting unknown anomalies often employ unsupervised or semi-supervised learning, relying on deviations from learned normal patterns.

Another classification of anomalies can also be proposed based on their characteristics:

Disruptive Signals: Jamming signals serve as a prime example of disruptive signals. Jamming signals, typically created by humans to interfere with a telecommunication system's receiver by transmitting high power, are referred to as jamming [26]. When jamming signals display known behavior, they are classified as known anomalies. Identifying these requires prior knowledge of various jammer types.

Some spectrum anomaly detection studies emphasize methods for detecting and classifying known types of jammers[27, 28]. However, real-world scenarios present the challenge of unknown jamming attacks[12, 13, 29]. These attacks are excluded from pre-existing algorithms, leaving such systems vulnerable.

Compiling a comprehensive database of all potential jamming attacks is challenging since new attacks can be easily generated by altering parameters like frequency, duration, or power. Consequently, numerous studies have aimed to identify spectral anomalies caused by unknown attacks. These methods typically issue alerts when anomalies occur. This approach aligns with the core concept of anomaly detection, where any unknown factor causing disruption in the telecommunication system is identified as an anomaly [30].

Interference: Anomalies such as interference, are unexpected events that disrupt telecommunication systems. Unlike jamming attacks, which are intentional, interference involves unintentional signals. Unlicensed frequency bands allow data transmission but face significant challenges from signal interference. For instance, interference between radar signals and LTE-U signals in the 5 GHz band in North America is a prominent example [19]. Detecting and managing interference as anomalies is a key area of research in cognitive radio[31].

B. System Model

The presence of spectrum anomalies can be modeled using a binary hypothesis framework as follows[32]:

$$H_0: y(n)=h(n)x(n)+N(n) \quad (1)$$

$$H_1: y(n)=h(n)x(n)+A(n)+N(n), n=1,...,w \quad (2)$$

Where $y(n)$ represents the received signal, $x(n)$ is the transmitted signal, $A(n)$ is the anomaly, $N(n)$ is the white noise with a Gaussian distribution and a two-sided power spectral density of $N_0/2$, and $h(n)$ is the channel coefficients. Also n refers to discrete time samples, and w is the length of the time window at the receiver. In Equation 2, $A(n)$ can be categorized into two types of anomalies: (1) anomaly signals or (2) unauthorized simultaneous signal activity within the frequency range of the authorized signal $x(n)$, referred to as interference [19]. Specifically, in spectrum anomaly detection using deep learning approaches, the acceptance or rejection of each hypothesis is carried out as follows:

$$\begin{aligned} &H_0 : F(P(y(n)))< \lambda : No\ Anomaly \\ &H_1 : F(P(y(n)))> \lambda : Anomaly\ present \end{aligned} \quad (3)$$

According to Equation 3, the received signal $y(n)$ is first preprocessed using a function P to extract relevant features and normalize the data. The preprocessed signal is then fed into deep learning models to learn a transformation function F. This function F is designed to map the input signal to a representation that emphasizes distinguishing features, enabling the model to detect anomalies effectively.

C. Performance Metrics for Spectrum Anomaly Detection

In anomaly detection, the following metrics are commonly used to assess the system's effectiveness[33]:

- Detection Probability (p_d): The probability of detecting an anomaly when an anomaly is present, denoted by:

$$p_d = p_r\{H_1 | H_1\} \quad (4)$$

- Miss Detection Probability (p_m): The probability that an anomaly goes undetected, denoted by:

$$p_m = p_r\{H_0 | H_1\} \quad (5)$$

- False Alarm Probability (p_f): The probability that a communication signal is mistakenly identified as an anomaly, denoted by:

$$p_f = p_r\{H_1 | H_0\} \quad (6)$$

- Receiver Operating Characteristic (ROC) Curve: A plot that shows the relationship between the p_f and the p_d for various Signal-to-Noise Ratio (SNR)values.

Furthermore, other evaluation criteria are used in spectrum anomaly detection to evaluate deep learning models, including the Dice Similarity Coefficient (DSC), Recall, Specificity, and Accuracy, are employed. These metrics are computed using Equations (7) to (10), respectively [34, 35]:

$$DSC = \frac{2TP}{2TP+FP+FN} \tag{7}$$

$$Recall = \frac{TP}{TP+FN} \tag{8}$$

$$Specificity = \frac{TN}{TN+FP} \tag{9}$$

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \tag{10}$$

3. Anomaly Detection Based Deep Learning

Deep learning methods, by capturing intrinsic patterns within data, have been extensively applied in cognitive radio tasks such as spectrum sensing[1, 36], signal classification[9, 37, 38], spectrum anomaly detection[12, 13, 29], and dynamic spectrum sharing[39]. Specifically, spectrum anomaly detection methods typically involve multiple stages, as illustrated in Figure 1. Initially, raw I/Q samples from the sensing frequency bands are captured. Depending on the sampling frequency, a specified number of samples are collected and represented $y[n]$ as a vector. These data vectors can then either be directly fed into deep learning models or undergo pre-processing to enhance their representation for further analysis. Pre-processing can be considered a crucial step in feature extraction, as it applies transformations to raw data, making it more suitable for analysis by emphasizing relevant patterns and reducing noise.

Once the pre-processing is completed, deep learning algorithms are employed to analyze the data. In intelligent spectrum management systems, these algorithms play a pivotal role in automating the detection and classification of wireless signals. At this stage, the focus is on identifying patterns within the processed data, enabling the model to learn task-specific features for applications such as modulation classification, wireless device identification, or anomaly detection. The following sections provide a detailed of the pre-processing techniques and deep learning models utilized in this context.

4. Pre-processing for Spectrum Anomaly Detection

Figure 2 shows that pre-processing for deep learning-based spectrum anomaly detection falls into four main categories: statistical features, sequence features, image-based features, and combined features. The following subsections provide a detailed overview of each approach.

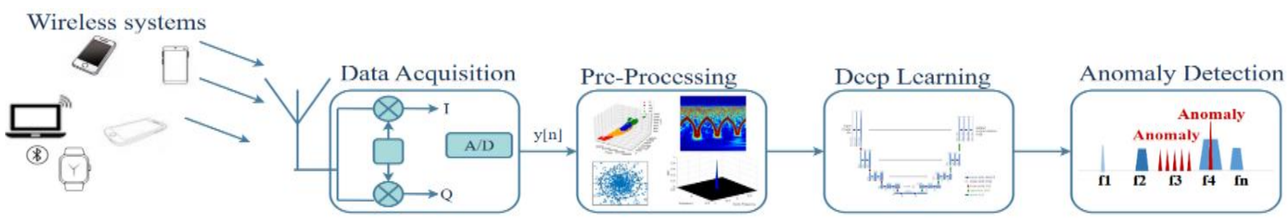


Figure 1: Overview of using deep learning models for spectrum anomaly detection.

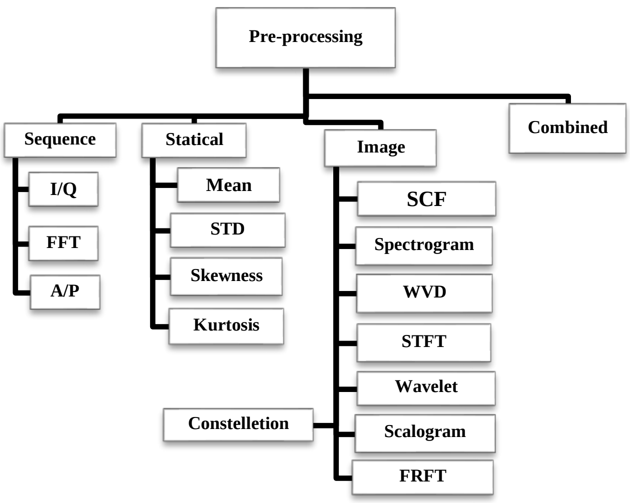


Figure 2: Pre-processing approaches for Spectrum Anomaly Detection

A. Sequence features

In this approach, the classification task is addressed based on the sequential processing of received samples:

I/Q: Specifically, the in-phase (I) and quadrature (Q) signal samples received from the receiver can be utilized directly for tasks such as modulation classification[37], and anomaly detection [18, 40]. Typically, the received samples are divided into fixed-length windows (for example 128 samples), and then fed into deep learning models. However, as the window length increases, the dimensionality of the input data also grows, necessitating the use of deeper models. Given the constraints of computational resources and processing time, some studies have proposed feature extraction techniques, such as applying Fast Fourier Transform (FFT) or deriving amplitude and phase vectors of the received signal, as an alternative to directly utilizing raw I/Q samples.

A/P: In addition to directly utilizing the raw I/Q samples, the amplitude (A) and phase (P) of the received samples can also serve as inputs to deep learning models by organizing them into two fixed-length windows. Compared to I/Q samples, the amplitude and phase representations demonstrate superior discrimination capabilities. This advantage arises from their inherent robustness to signal impairments, such as frequency shifts and phase variations, which can significantly impact the I/Q components. By leveraging this alternative representation, models can achieve improved performance in challenging signal environments[18].

FFT: Fast Fourier Transform (FFT) is commonly used in telecommunications, especially for spectrum sensing and anomaly detection, to convert received samples into the frequency domain. In this domain, frequency-related information proves highly effective for tasks where the frequency of occurrence is critical, such as identifying the frequency range occupied by communication signals. The FFT output, which consists of real and imaginary components, can be directly utilized as input to deep learning models. Selecting an appropriate number of FFT points is a key consideration; fewer FFT points reduce computational complexity, whereas a larger number increases computational demands[18, 41].

B. Statical Features

Various statistical features can be used in the task of spectrum anomaly classification [42]. These features are also widely utilized in other telecommunications applications, such as signal detection, modulation classification, and related tasks. Below are some of the most commonly employed statistical features [3, 34, 15]:

Mean: Represents the average signal value, providing insight into the signal's general level or bias[43].

Standard Deviation (STD): Measures variability around the mean, indicating signal fluctuations[44].

Skewness: Reflects the asymmetry in the signal's distribution, useful for detecting non-Gaussian interference[45].

Kurtosis: Measures the tailedness of the distribution, often helpful for identifying anomalies that introduce extreme values[46].

These basic statistical features offer simple and efficient computation. However, they lack the ability to localize anomalies in time or frequency. Therefore, for anomaly localization, transformations such as FFT, power spectral density (PSD), and time-frequency representations are commonly employed.

C. Image-based features

Deep learning excels in computer vision tasks like detection, classification, and segmentation by automatically extracting relevant features from image inputs[47]. Similarly, in telecommunications systems, received signals can be transformed into time-frequency representations by applying appropriate processing techniques. The subsequent sections explore some of these processing methods in detail:

SCF: This processing technique enables the effective extraction of periodic patterns from received signals. The concept of periodicity encompasses symbols, spreading codes, and guard intervals. Some signals exhibit unique periodic or cyclostationary characteristics. By analyzing these cyclostationary features, it becomes possible to identify the type of received signal without prior knowledge, even under challenging conditions such as noise and multipath fading effects. Assuming a fundamental periodicity $T_0 = \frac{1}{f_0}$, the cyclic autocorrelation function $R_y^{\alpha}(\tau)$ at cyclic frequency α is obtained. Applying the Fourier transform to the CAF yields the Spectral Correlation Function (SCF), as defined in Equation (11) [48]:

$$S_y(f) = \int_{-T/2}^{T/2} R_y^{\alpha}(\tau) e^{-j2\pi f \tau} d\tau \tag{11}$$

Where $\alpha = 0$, $S_y(f)$ represents the power spectral density (PSD) function [13, 49]. The computational complexity of the SCF is relatively high compared to alternative methods. To address this, Kürşat, et al. [48]reduce the SCF complexity by employing FFT-based accumulation methods (FAM), utilizing time smoothing via the FFT. Figure 3 represents an example of SCF estimation using the FAM algorithm for three signal types, UMTS, GSM, and LTE, along with AWGN. As illustrated in the Figure 3, each signal demonstrates unique cyclostationary properties, whereas AWGN lacks these characteristics, showing a single non-zero peak in SCF at the center of the frequency domain.

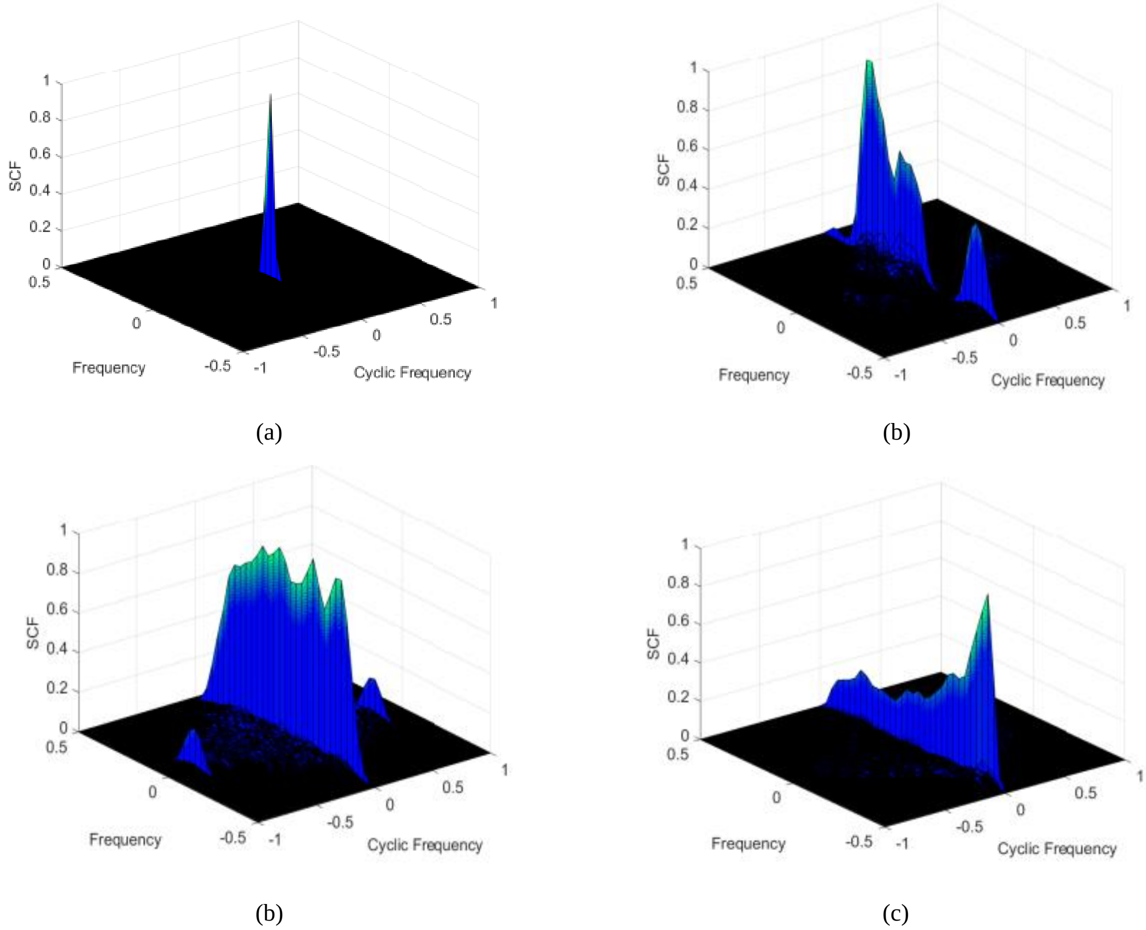


Figure 3: Estimation of the SCF using the FAM algorithm for a) AWGN, b) GSM, c) UMTS, and d) LTE[48].

STFT & spectrogram: The short-time Fourier transform (STFT) and the spectrogram are closely related, with the spectrogram being derived from the magnitude of the STFT. Unlike separate time-domain or frequency-domain analyses, the spectrogram provides a combined view, enabling the association of maximum energy values with both temporal and frequency components [32, 50, 51]. Spectrogram computation involves segmenting the signal with a window function and applying the FFT to each segment [12, 19, 27, 29, 45, 52-58]. As illustrated in Figure 4, the spectrogram effectively detects time-varying anomalies such as chirp signals, while also distinguishing different types of communication signals based on their time-frequency characteristics. The choice of frame length and the number of FFT points directly affects the trade-off between time and frequency resolution. Increasing the FFT size improves frequency resolution but also raises computational complexity. To address this issue, [19]introduces a modified version of the spectrogram, called the Q-spectrogram. The Q-spectrogram is designed to optimize the representation of time and frequency information while reducing input complexity for CNN models. It is generated by condensing a standard spectrogram (e.g., 128 × 128 or other sizes) into a smaller, quarter-sized representation.

Wavelet & Scalogram: The wavelet transform is another representation for time-frequency analysis of received signals. Unlike the STFT, which uses a fixed-length window, the wavelet transform utilizes a base function, known as the mother wavelet, with varying scales and shifts as it moves across the signal This allows for the capture of time and frequency information at different resolutions, making wavelets particularly well-suited for analyzing non-stationary signals[60, 61]. Since real-world signals are typically discrete, the Discrete Wavelet Transform (DWT) is commonly used for analysis.

Complementing the wavelet transform, the scalogram provides a time-frequency representation of the received signal samples. Specifically, it is derived by calculating the squared magnitude of the CWT. Ujan et al.[62] used deep learning models for identifying types of interference in satellite-to-ground real-time communication within the DVB-S2 standard with the benefit of scalogram. Figure 5 illustrates examples of scalograms for signals with interference. As shown, this transform is particularly effective in distinguishing different types of interference, especially chirp-type interference [46, 63].

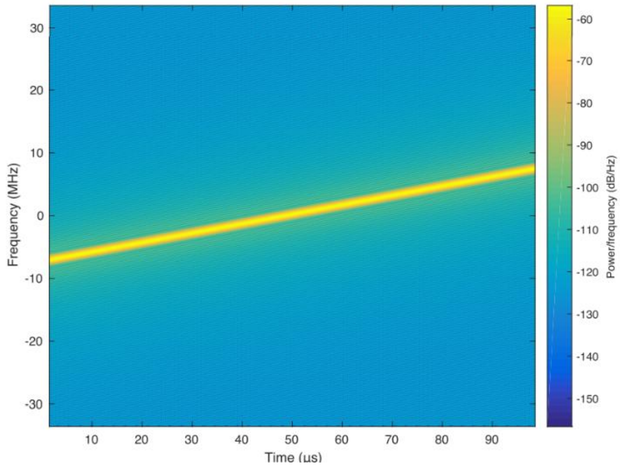


Figure 4: Illustrative example of the spectrogram for a chirp anomaly[59].

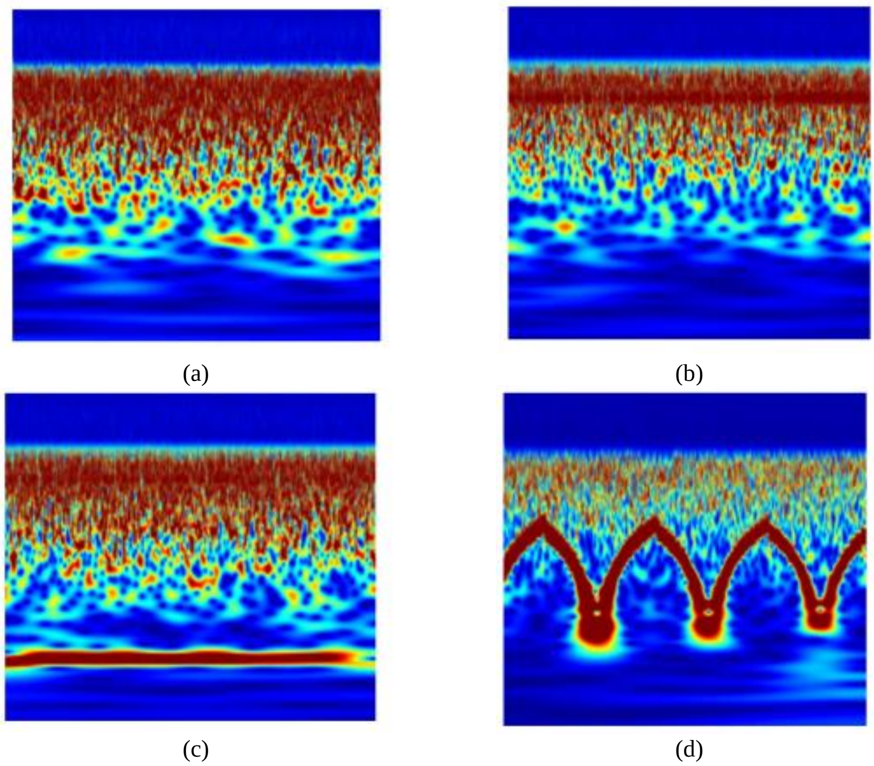
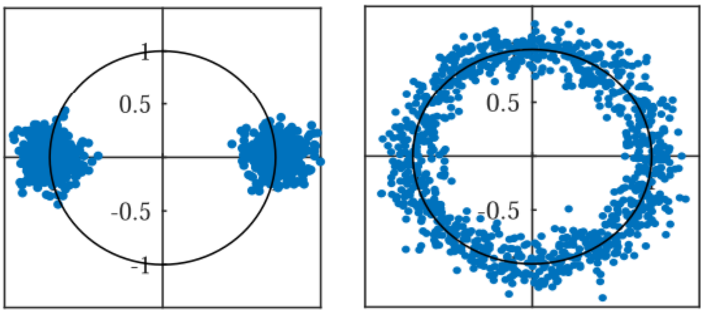
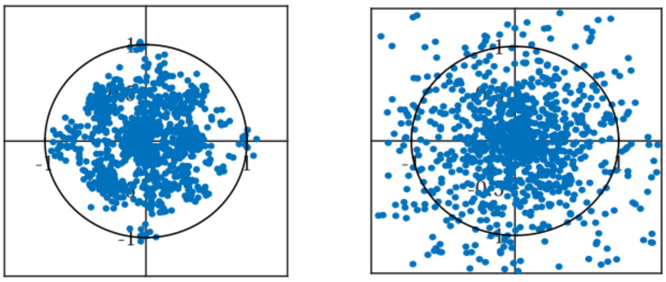


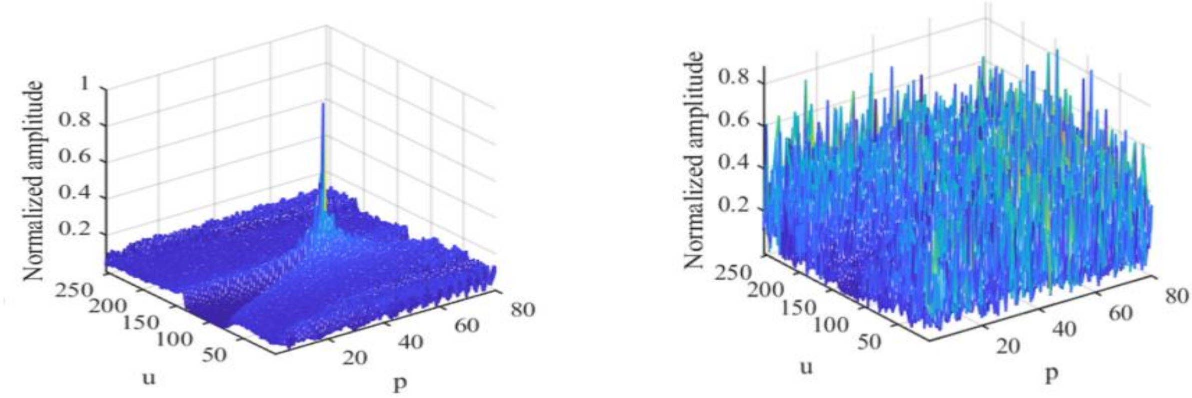
Figure 5: Scalogram representation of received signals in satellite communication based on the DVB-S2 standard, illustrating a) signal without the interference, b) Signal with single-tone interference, c) signal with multi-tone interference, and d) signal with chirp interference [46].





(c) (d)

Figure 6: Representation of Anomaly Types: a) Random Binary Code Anomaly, b) Single-Tone Anomaly, c) Multi-Tone Anomaly, and d) Partial Frequency Band Noise anomaly [28]



(a) (b)

Figure 7: Example of the FRFT representation for, a) chirp signal, b) non-chirp signal [28]

Constellation: The constellation diagram allows for the visualization of the scatter of I/Q samples in the received signal, and is commonly used for modulation classification and anomaly detection [37, 43, 44]. For example, Figure 6 presents constellation diagrams for samples of various anomalies. According to this figure, signal points in single-tone and binary code anomaly are symmetrically distributed around the unit circle, whereas multi-tone and frequency band noise anomaly exhibit more irregular patterns. These characteristics enable the identification of deceptive anomaly based on the dispersion of signal points around the circle's center [28]. While the constellation diagram provides valuable insights, its effectiveness in classification diminishes at low SNR levels.

WVD: The Wigner-Ville distribution (WVD) is a second-order time-frequency distribution that maps a signal from the time domain to the energy density plane[28, 64]. The Wigner distribution of a signal y(t) is calculated based on the Fourier transform of its instantaneous autocorrelation function, as shown in the Equation 12:

$$WVD_y(t,\omega)=F_{\tau\to\omega}\left\{y\left(t+\frac{\tau}{2}\right)y^*\left(t+\frac{\tau}{2}\right)\right\} \quad (12)$$

The resulting Fourier transform is real-valued in the Hermitian space, and therefore, cross-terms appear in the output. In fact, the Wigner distribution generates cross-terms between the positive and negative frequencies of the main signal. To discard these cross-terms, the Wigner-Ville distribution and its modified version, the Smooth Pseudo Wigner-Ville Distribution (SPWVD) [65], are introduced. Instead of computing the Wigner-Ville distribution directly for the signal, the Wigner-Ville distribution of the corresponding analytic signal is calculated. The analytic signal corresponds to the main signal but contains only non-negative frequencies. Using this analytic signal helps remove some of the external cross-terms.

FRFT: The fractional Fourier transform (FRFT) is an extension of the conventional Fourier transform that rotates the time-frequency plane by a specific angle. It represents a signal using a set of orthogonal bases and is particularly effective for detecting chirp signals. To do so, a parameter is adjusted until the transform aligns with the target chirp pattern. As illustrated in Figure 7, the energy of a chirp signal becomes concentrated at a specific value, while in non-chirp signals, the energy remains more dispersed[28].

D. Combined features

This approach enables the integration of features outlined in previous sections as input to deep learning models[54, 66]. Although this increases computational overhead, it can potentially improve the accuracy of anomaly detection. Suppressive anomaly, such as tone, multi-tone anomaly, and chirp anomaly, disrupt

communication by transmitting high-power signals, while deceptive anomaly mimic legitimate signals to exploit frequency bands. Liu et al. [28] proposed using constellation diagrams, WVD, and FRFT to detect and classify both types of anomalies. Their study shows that WVD is effective for suppressive anomalies, and FRFT is more suited for chirp anomalies, while constellation diagrams can detect both types.

Ujan et al. [46] used 10 statistical and wavelet-based features to classify modulation schemes and detect signal of interest (SOI), continuous wave interference (CW), multiple continuous wave interference (MC), and chirp interference (CI). An example showing three wavelet coefficients across four levels for these classes is illustrated in Figure 8. These extracted features contribute significantly to distinguishing between different types of interference.

E. Comparison of Pre-processing Techniques

Table 2 provides a comparison of various pre-processing techniques in terms of anomaly detection performance, localization capability, and computational complexity. Sequence-based methods and statistical features are computationally efficient but lack time-frequency resolution. Time-frequency methods such as STFT and spectrogram offer improved anomaly detection and localization by preserving the temporal-spectral structure. While advanced transforms such as SPWVD, WVD, and FRFT provide higher resolution and are effective for chirp detection, they introduce greater computational complexity.

The choice of pre-processing also affects the model architecture. Image-based features typically require deep 2D Convolutional Neural Networks (CNNs) for effective representation learning, increasing computational demands. In contrast, simpler features such as PSD or FFT can be processed with traditional machine learning methods, offering a more efficient and lightweight solution. Hence, details related to deep learning models will be discussed in the following section.

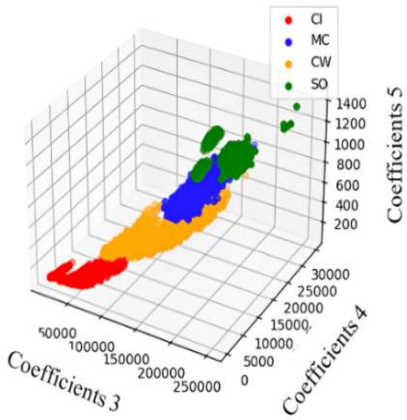


Figure 8: Illustration of the wavelet level-4 coefficients for signals with and without interference.

TABLE 2
Comparison of Pre-processing Techniques for Spectrum Anomaly Detection

References	Pre-processing		Capability	Computational Complexity
[40]	Sequences	I/Q sequences for feature extraction	Detection	Low
[41]		FFT	Detection	Moderate (depends on FFT points)
[13, 49]		PSD	Detection/Localization	Moderate (depends on FFT points)
[46]	Statistical	Mean, standard deviation, skewness, Real-Signal Kurtosis, average power, and average power of the wavelet coefficients	Detection	Low
[42]		Pseudo-range, Carrier phase, Doppler shift, Signal strength	Detection	Low
[32, 50, 51, 55]	Image-based	STFT	Detection/Localization	Moderate (Depends on FFT size)
[12, 27, 29, 45, 52, 53]		Spectrogram	Detection/Localization	Moderate (Depends on FFT size)
[19]		Q-spectrogram	Detection	Moderate (smaller size reduces complexity)
[62, 63]		Scalogram	Detection	High (due to CWT computations)
[65]		SPWVD	Detection	High
[54]	Combined	Spectrogram, PSD, raw constellation plots, and histogram	Detection	High
[66]		PSD, I/Q sequences	Detection	Moderate(depends on FFT points)
[28]		SPWVD, FRFT, constellation diagram	Detection	High
[18]		I/Q, amplitude/phase, FFT	Detection	Moderate (depends on FFT points)

5. Application of Deep Learning for the Spectrum Anomaly Detection

Research on spectrum anomaly can be classified into five main categories based on their application: reconstruction, recognition, classification, object detection, and segmentation approaches. In reconstruction-based approaches, where the nature of the anomaly is assumed to be unknown, the spectrum monitoring system can only detect the presence or absence of an anomaly and issue an alert. Some studies shift their objective to identifying known types of anomalies, which requires classification or recognition-based methods. In both classification and recognition approaches, the problem is addressed by predefining the number of known anomaly classes. Other studies also focus on the time-frequency occurrences of anomalies in addition to detecting their class. For this purpose, segmentation models or object detection models are employed, utilizing time-frequency representations. The following section provides a more detailed discussion of each approach.

A. Classification & Recognition-Based Anomaly Detection

Deep learning models can be used to classify types of spectrum anomalies. According to Figure 9, for multi-class classification tasks, the input is classified into one of the predefined classes. Some studies in this approach have introduced specific CNN-based models. For example, Morales Ferre et al. [27] proposed a lightweight CNN to classify types of jammers and legitimate signals within satellite-based Global Navigation Satellite Systems (GNSS). Their CNN processes grayscale spectrograms and consists of convolutional layers, pooling, and a fully connected layer for classification. The proposed algorithm achieved a classification accuracy of 91.36% on the test dataset. Similarly, Davaslioglu et al. [40] designed the DeepWiFi protocol for jamming detection in multi-hop wireless networks. It uses deep CNNs and feedforward neural networks (FNNs) and achieves over 98% accuracy, much higher than traditional methods like SVM with 66%. This helps users avoid interference, improving transmission speeds and data security. Xu et al. [41] applied the Spectrum Learning Anomaly Detection (SLAD) system based on CNNs, to detect normal communication, abnormal data, or interference in the 5G-Unlicensed spectrum (5G-U). The SLAD system applies FFT transformations to I/Q samples and achieves a classification accuracy of 97.6%. Kulin et al.[18] used CNNs and three data representations including IQ, amplitude/phase, and frequency domain for interference detection and modulation recognition. The framework achieves up to 86% accuracy in modulation recognition under high SNR and 98-99% in interference detection.

Some other studies in anomaly detection concentrate on employing well-known architectures that have been successfully applied in computer vision tasks. In this regard, Bhatti et al. [19] used several well-known CNN architectures, including Visual Geometry Group (VGG) [67] and Residual Networks (ResNet) [68], and SqueezeNet [69], to classify 10 signal types (e.g., LTE, WiFi, radar, filter bank multicarrier) and their respective interferences and noise.The VGG model is known for its deep but computationally heavy structure, ResNet introduces skip connections to ease training, and SqueezeNet achieves comparable accuracy with significantly fewer parameters. Using Q-spectrograms as input, they showed that ResNet18 and SqueezeNet outperformed traditional methods in terms of both speed and accuracy.

Swinney et al.[54] utilized unsupervised learning techniques to address the challenge of GNSS jamming signal detection and clustering. Their approach involved leveraging graphical representations of radio frequency signals, including spectrograms, power spectral density, raw constellation plots, and histograms. They used the VGG-16 model with transfer learning for feature extraction, which enhanced the accuracy and efficiency of k-means clustering. Experiments with different initialization methods confirmed the advantage of CNN features, while also reducing processing time, making the approach suitable for early warning systems. Similarly, Jiang et al. [53] proposed a VGG-16-based framework for GNSS interference classification using federated and transfer learning. Time–frequency spectrograms were used as input, enabling decentralized training with improved privacy and faster convergence. Results showed that the untrained VGG-16 model achieved 96.7% accuracy, outperforming conventional CNNs by 8%. Steiner et al. [52] used five ResNet models (ResNet-18 to ResNet-152) to classify seven types of GNSS jamming signals based on spectrogram images. The best performance was achieved with ResNet-152 (accuracy of 94%), while ResNet-18 offered a good trade-off between accuracy (91.4%) and speed.

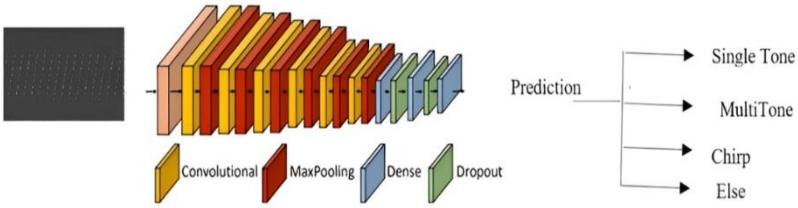


Figure 9: Illustrating the Application of Deep Learning Models in Classifying Intentional Interference

In recent years, a growing number of studies in the field of anomaly detection have adopted architectures designed to process sequential data. These architectures offer significant advantages, such as the ability to model long-range dependencies and to selectively focus on the most informative aspects of the input, thereby enhancing the accuracy and robustness of anomaly detection systems. For example, Reda et al.[42] developed a deep learning method for detecting GNSS jamming using time-series features from RINEX data. After PCA and Bayesian Optimization for feature selection, they trained LSTM-based models. The BiLSTM-A model, enhanced with an Attention Mechanism to focus on key time steps, achieved 98.08% accuracy in detecting chirp and CW jamming. Results highlight the effectiveness of attention-based RNNs in GNSS interference detection.

Table 3 provides a comprehensive comparison of key methods in spectrum anomaly detection and classification, highlighting their accuracy, strengths, and limitations. Based on this comparison, several practical implications can be identified:

Speed vs. Accuracy Trade-offs: Lightweight models such as ResNet-18 and SqueezeNet provide faster inference times, making them suitable for real-time or resource-constrained applications. In contrast, deeper architectures like ResNet-152 offer higher accuracy but require significantly more computational resources, which may restrict their use in latency-sensitive environments.

Pre-processing-Impact of Input Representation: Models operating on raw or time-series data, including BiLSTM-based architectures, typically require larger, high-quality datasets and longer training durations to achieve optimal performance.

Generalization: Protocol-specific models (e.g., DeepWiFi) or domain-focused approaches targeting only GNSS signals may have limited generalization capability when applied beyond their original context, necessitating domain adaptation or retraining.

Robustness: Approaches that incorporate spectral transformations (e.g., spectrograms, FFT) and attention mechanisms generally exhibit greater robustness against noise and variability, which are common in real-world signal environments.

B. Object Detection-Based Anomaly Detection

Object detection tasks focus on predicting both the class and approximate location of an object within input data. Notable models in this domain include Region-based Convolutional Neural Network (R-CNN) [70], Fast R-CNN[71], Faster R- CNN [72], and the You Only Look Once (YOLO) family [73-75]. Object detection models are also applicable to spectrum anomaly detection tasks, enabling simultaneous detection and localization of spectrum anomalies. Advanced architectures, such as those introduced by Qin et al. [55] demonstrate the effectiveness of deep learning-based interference monitoring systems. According to Figure 10, their proposed deep learning architecture employs a CSPDarknet-based backbone network for feature extraction, spatial pyramid pooling for feature integration, and PANet to enhance multi-scale object detection. El-Haryqy et al. [63] introduced a novel approach for joint radio frequency interference detection and automatic modulation recognition using Mask R-CNN. Unlike traditional object detection methods that rely only on bounding boxes, this approach leverages instance segmentation to generate precise pixel-level masks for each type of interference and modulation, enabling more accurate and detailed recognition. Kim et al. [51] proposed an object detection-based approach for wideband anomaly detection using STFT spectrograms of LTE and 5G signals. Unlike prior narrowband-focused studies, this work targets wideband signals. Using models like YOLOv11 and RT-DETR, they achieved up to 93.7% accuracy.

TABLE 3
Comparison of Deep Learning Models for Spectrum Anomaly Classification

Reference	Model	Pre-processing	Accuracy (%)	Strengths	Limitations
Morales Ferre et al. [27]	CNN	Grayscale Spectrogram	91.36	Good accuracy, simple model	Limited generalization
Davaslioglu et al. [40]	CNN + FNN	Raw Signal	>98	High accuracy, improves throughput	Network-specific
Bhatti et al. [19]	ResNet18, SqueezeNet	Q-spectrogram	~95	Efficient input size, fast inference, robust in multi-signal environments	Potential loss of fine spectral details
Xu et al. [41]	CNN	FFT-normalized I/Q	97.6	Robust in noisy industrial settings	Not evaluated on other spectra
Kulin et al.[18]	CNN	Raw spectrum (IQ, amplitude/phase, frequency domain)	98-99%	End-to-end learning from raw data, multiple representations improve performance	Needs high SNR for best results
Swinney et al.[54]	VGG-16+ Unsupervised	Various RF signal representations	-	Improved clustering, efficient, suitable for early warning	Binary classification only
Steiner et al. [52]	ResNet (18 to 152 layers)	Spectrogram	91.4 - 94	Accurate, diverse jamming types	Trade-off speed vs. accuracy
Reda et al.[42]	BiLSTM + Attention	Time-series RINEX	98.08	High accuracy, temporal dependency capture	Computationally intensive
Jiang et al. [53]	VGG-16	Spectrogram	96.7	High accuracy, privacy-preserving, decentralized training, fast convergence	Computationally intensive

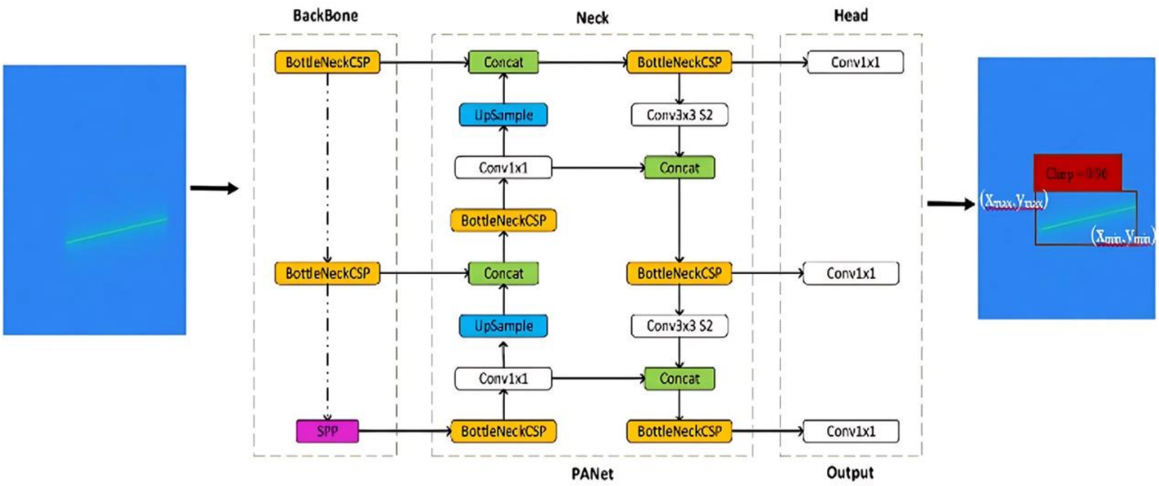


Figure 10: Illustrating the Application of Deep Learning Models in spectrum anomaly detection. The model's architecture, as well as its inputs and outputs, belong to [55].

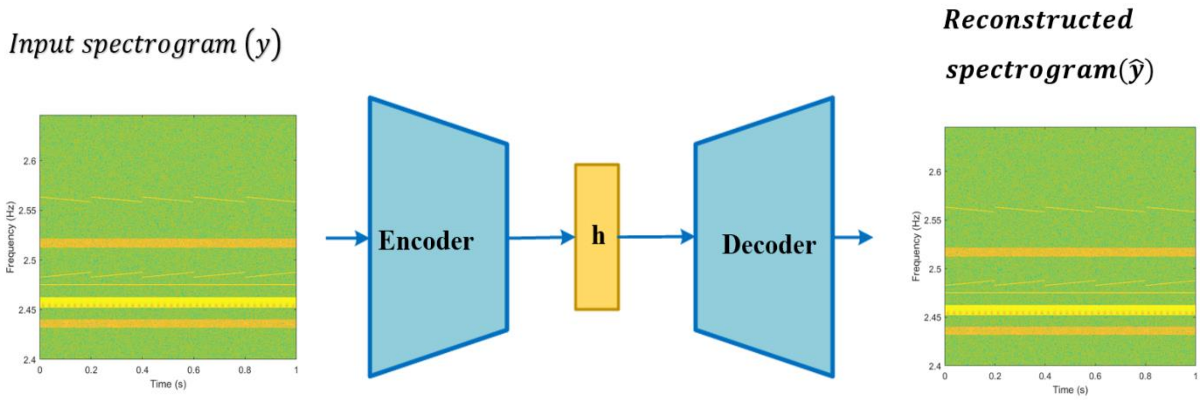


Figure 11: Illustrating the Application of Deep Learning Models in reconstruction-Based spectrum anomaly detection.

C. Reconstruction-based Anomaly Detection

Autoencoders (AEs) are a widely used deep learning model in reconstruction-based approaches and are particularly effective for anomaly detection tasks [76]. In these tasks, the model learns to compress input data into a lower-dimensional latent space while preserving its essential features and then reconstructs the data back to its original size. As shown in Figure 11, an autoencoder consists of three main components: the encoder, the bottleneck, and the decoder. The encoder transforms the input data into a compact representation in the bottleneck by reducing its dimensionality, learning patterns from the training samples without prior knowledge of the data distribution. The bottleneck represents the compressed latent space, where the most significant features of the data are retained. The decoder then reconstructs the original data by learning the inverse transformation from the compact representation during training. This process enables the model to effectively capture intrinsic patterns in the data, making it particularly well-suited for identifying anomalies [15, 45, 77].

Let y denote the selected input points within a range of length w. The encoding and decoding processes of the autoencoder are formally represented by Equations (13) and (14), respectively [15]:

$$Z_{t-w:t} = E(y,\phi) \tag{13}$$

$$y_{t-w:t} = D(Z,\theta) \tag{14}$$

Where Z represents the learned representation of the input within the bottleneck, while $\hat{y}$ denotes the reconstruction of y. The encoder and decoder components are denoted by E and D, respectively, and are parameterized by $\emptyset$ and θ. During the training process, the parameters of both components are optimized by minimizing a loss function that quantifies the reconstruction error between the original data and its reconstruction, as specified in Equation (15) [15, 45, 77]:

$$\left(\phi^*,\theta^*\right) = \arg\min_{\phi,\theta} Err\left(y, D\left(E\left(y,\phi\right),\theta\right)\right) \tag{15}$$

For anomaly detection tasks, the autoencoder is trained exclusively on normal data. This training process enables the autoencoder to learn the inherent patterns of the normal data effectively, resulting in a significantly lower reconstruction error for normal samples. However, when anomalous data is presented, the reconstruction error increases noticeably. By defining an appropriate threshold, these anomalies can be identified. This threshold, often referred to as the anomaly score (AS_w) is computed using Equation (16):

$$AS_w = \left\| y - D(E(y,\phi),\theta) \right\|^2 \quad (16)$$

Determining an appropriate anomaly score in this method is a critical challenge. Feng et al. [50] proposed a novel approach for calculating the threshold in anomaly detection for wireless spectrum monitoring. They defined a dynamic thresholding method that traverses from the maximum reconstruction error of normal samples to the minimum error of anomaly samples, optimizing the threshold for improved performance .Their results showed that deep autoencoders significantly outperformed shallow networks and traditional methods, achieving 88.57% accuracy with a four-layer model at an SNR of 20 dB. Similarly, Rajendran et al. [13] employed a dynamic thresholding approach at the output of the Adversarial Autoencoders(AAE) model, where thresholds were adaptively adjusted using n-sigma rules based on the mean and standard deviation of the training data. This strategy ensured robust anomaly detection performance under diverse datasets and noise levels.

Some studies have focused on enhancing the architecture of autoencoders to improve anomaly detection performance in wireless spectrum analysis. For instance, Zhou et al. [32] developed a modified Generative Adversarial Network (E-GAN) using STFT-based spectrograms to detect and localize four jammer types, combining reconstruction error and discriminator loss for robust detection. Similarly, Toma et al. [58] employed deep generative models including Conditional GAN (C-GAN), Auxiliary Classifier GAN (AC-GAN), and Variational Autoencoder (VAE) on Stockwell-transformed spectrum data in mmWave systems. AC-GAN achieved the highest detection rate, while VAE offered faster computations, balancing accuracy and efficiency. Zeng et al.[66] presented an enhanced anomaly detection framework by integrating Autoencoder architecture with Denoising Diffusion Probabilistic Models (AE-DDPMs). By operating in a low-dimensional latent space, the model improves efficiency and stability over traditional DDPMs. It avoids issues of adversarial training and achieves better low-SNR performance, outperforming E-GAN by 8 dB in the term of detection accuracy. The approach uses I/Q data and PSD features to detect various jamming signals, including AM, FM, tone, and chirp types.

Traditional autoencoders face several limitations in spectrum anomaly detection. A significant issue is over-recovery, where anomalous signals are reconstructed as normal, leading to reduced anomaly scores and impairing the model's ability to distinguish between normal and abnormal data. Additionally, traditional models often struggle to generalize in dynamic and noisy environments due to their inability to capture long-range dependencies and complex patterns in spectral data. These challenges are further compounded by their computational demands and susceptibility to errors in anomaly localization, which limits their effectiveness in practical applications. To address these limitations, Huang et al. [29] proposed a novel architecture based on Masked Autoencoders (MAE). This approach leverages a masking mechanism and the Multi-Head Self-Attention (MHSA) framework to enhance the model's ability to focus on reconstructing critical features of normal data, improve anomaly detection and localization accuracy, and ensure robustness across diverse datasets and noise conditions.

Additionally , Qi et al. [12] introduced the Unsupervised Deep Memory Autoencoders (UDMA) framework, which enhances traditional autoencoder methods using a teacher-student architecture with memory modules and knowledge distillation. A teacher extracts features from normal signals, while two student networks (one memory-based) learn to replicate these outputs. Anomalies are detected based on discrepancies between teacher and students. UDMA achieved over 85% recall even under low SNR conditions. Similarly, Kuang et al.[65] introduced an Improved Memory-Augmented Autoencoder (IIMemAE) to detect abnormal signals. It integrates an encoder-decoder structure, a memory module for normal pattern storage, and a refined anomaly detection method (parametric Pauta criterion). The model achieved a high AUC of 95.49%, effectively handling imbalanced datasets and redundant spectrogram information.

Another approach to capturing dependencies among data is the use of attention mechanisms, which are considered a type of memory-based architecture. In this context, Liu et al. [49] proposed an unsupervised VAE-based model with an adaptive attention mechanism to detect spectrum anomalies from one-dimensional PSD data. The model suppresses noise floor effects and enhances signal features using learned thresholds and attention weights, and it outperformed E-GAN, especially in low ISR scenarios.

The probability of detection at a fixed Probability of false alarm is commonly used as a performance metric for evaluating reconstruction-based spectrum anomaly detection methods. Accordingly, Table 4 provides a comparative analysis of various approaches, highlighting their respective advantages and limitations. Based on this

comparison, several practical implications can be identified:

Detection Performance vs. Complexity: Recent autoencoder designs increasingly employ attention mechanisms and memory modules, yielding higher detection accuracy, especially under low SNR and imbalanced data. However, these gains come with greater computational cost and tuning requirements.

Pre-processing-Impact of Input Representation: Employing advanced time-frequency representations, such as the SPWVD used by Kuang et al. [65] or spectrograms as in Zhou et al. [32], facilitates the extraction of hidden signal patterns, thereby improving anomaly detection performance. Nonetheless, these approaches require computationally intensive pre-processing steps. Simpler input forms, for example, direct PSD inputs, reduce pre-processing overhead and enable faster implementations but may slightly compromise sensitivity to specific anomaly types.

Robustness to Noise and Interference Suppression Ratio (ISR) Conditions: Models integrating attention mechanisms[29] or memory modules [65] demonstrate enhanced capability to differentiate anomalies from noise, contributing to more stable performance in realistic environments characterized by low ISR. Similarly, the diffusion-based approach in AE-DDPM[66] exhibits superior noise resilience and greater stability compared to GAN-based models, owing to its probabilistic generative framework in the latent space.

Thresholding Strategies and Anomaly Scoring: Determining optimal anomaly detection thresholds remains a fundamental challenge. Dynamic thresholding methods[13, 50], leverage statistical properties of reconstruction errors (e.g., standard deviation or median error) derived from training data. More advanced models[29, 66], utilize hybrid scoring mechanisms combining reconstruction error with attention-weighted metrics or learnable thresholds, enhancing adaptability to novel data distributions.

Model Scalability and Real-World Applicability: Autoencoder variants like AAE or VAE feature modular architectures conducive to scalability and generalization across diverse datasets and operational contexts. Conversely, GAN- or diffusion-based models demand higher computational resources, posing challenges for real-time deployment and implementation on hardware with limited capabilities.

TABLE 4
Comparison of Deep Learning Models for Reconstruction-based Anomaly Detection

Reference	Model	Pre-processing	P_d /Recall(%)	Strengths	Limitations
Feng et al. [50]	Autoencoder	STFT	-	Dynamic threshold	Sensitive to threshold selection, requires fine tuning
Rajendran et al. [13]	AAE	PSD of synthetic and real signals	> 80% at a constant false alarm rate of 1%	Dynamic threshold	Model complexity, dependency on threshold parameters
Zhou et al. [32]	E-GAN	Spectrogram	75-95 at a constant false alarm rate of 0.01% 85-98 at a constant false alarm rate of 0. 1% 95-100 at a constant false alarm rate of 1% Close to at a constant false alarm rate of 10%	Improved over Basic AE, Combines reconstruction and discriminator errors, detects multiple jammer types	Sensitive to training data, training complexity
Toma et al. [58]	Conditional GANs and VAE + Stockwell Transform	mmWave data with generalized state vectors	-	Improved over Basic AE, Balance between accuracy and speed, diverse models,	Complexity and resource intensive
Zeng et al.[66]	AE-DDPM	PSD + I/Q sequences	-	Improved over Basic AE, More stable, lower resource consumption	Requires fine tuning, relatively new model
Huang et al. [29]	MHSA	Spectrogram	87.99% at a constant false alarm rate of 5%	Memory-Based Mechanism Enhanced ,Focus on important features	Computational complexity
Qi et al. [12]	UDMA	Spectral and time-frequency data	Close to100 at a constant false alarm rate of 1% for the ISR>0dB	Memory-Based Mechanism Enhanced ,Teacher-student architecture, robust to noise	Model complexity, requires careful training
Kuang et al.[65]	IIMemAE	SPWVD	70-85 at a constant false alarm rate of 1% for the ISR>0dB [12]	Memory-Based Mechanism Enhanced , Reduces redundant information, high performance on imbalanced data	High complexity, heavy pre-processing
Liu et al. [49]	VAE + adaptive attention mechanism	One-dimensional PSD	Close to100 at a constant false alarm rate of 1% for the ISR>0dB	Memory-Based Mechanism Enhanced , High sensitivity, superior performance in low ISR noise	Model complexity

D. Segmentation-Based Anomaly Detection

Segmentation is a process in which the input is divided into distinct regions, with each region representing an object or area whose components share similar characteristics. This approach not only identifies the presence of objects but also pinpoints their boundaries. In contrast to classification, which assigns a single label to an entire input (e.g., an image or a spectrogram), segmentation operates at a finer granularity by classifying each individual pixel or element of the input into one of the predefined classes. The input and output of a deep learning model for segmentation tasks typically have identical dimensions, ensuring that each element of the input is mapped to a corresponding classification in the output. Commonly, encoder-decoder architectures are utilized to address such tasks due to their ability to capture hierarchical features while maintaining spatial or spectral resolution.

While object detection models estimate the approximate range of signals, segmentation methods provide more precise localization and classification of signals. For spectrum anomaly detection task, it is possible to use a hybrid approach based on reconstruction and segmentation. For example, Peng et al. [45] proposed a spatio-temporal framework that integrates CNNs and LSTM modules to predict spectrum data and identify anomalies. The proposed approach processes the historical spectrum data at multiple timescales (e.g., short-term, hourly, daily) using a sliding window technique and employs deep networks to learn spatio-temporal features. Although the primary task focuses on prediction, the framework indirectly resembles segmentation by mapping each frequency-time segment of the spectrum to either normal or anomaly. By combining aspects of reconstruction and segmentation, this hybrid model achieves robust and precise anomaly detection, demonstrating superior performance in multi-signal, wideband spectrum sensing scenarios.

6. ANALYSIS OF SPECTRUM ANOMALY DETECTION APPROACHES

A. Comparison of Methods

Table 5 provides a summary of research conducted on spectrum anomaly detection. In deep learning applications, it is crucial to first define the problem-solving approach, whether classification, segmentation, or object detection, and then select models that align with the chosen method. As highlighted in Table 5, spectrum anomaly detection can be approached through various methodologies. Reconstruction-based method [12, 13, 29, 32, 49, 50, 58, 65, 66] approaches are predominant in the literature, as they enable models to identify and localize unknown anomalies. A significant challenge in these methods lies in selecting an optimal threshold. Consequently, as previously discussed, several studies have proposed dynamic thresholding techniques to address this issue. Alternatively, for classifying known anomalies such as tone, multi-tone, and chirp, methods based on object detection[51, 55], classification [18, 19, 27, 40-42, 46, 52-54, 62], recognition[28], or segmentation are more suitable. Among these, models for segmentation [45] and object detection [51, 55, 63] provide the benefit of enabling both localization and classification of anomalies simultaneously.

From another perspective, classification and recognition-based methods are more effective for detecting anomalies in narrowband spectrum sensing. Conversely, segmentation, and object detection approaches are more appropriate for wideband spectrum sensing scenarios, where multiple communication signals and anomalies may occur simultaneously.

Comparisons indicate that in spectrum anomaly detection across classification, reconstruction, and other approaches, models based on convolutional neural networks have dominated due to their effective feature extraction. Recently, memory-based models utilizing attention mechanisms have attracted significant interest because they better capture long-term dependencies and complex temporal patterns in spectral data, leading to improved detection of subtle and dynamic anomalies.

B. Current Challenges & Future Directions

One of the critical challenges in applying deep learning models for spectrum anomaly detection is obtaining a diverse and high-quality dataset for effective model training. Table 5 presents a comparison of existing datasets based on two key factors: availability and the nature of the data (real or synthetic). As illustrated, the majority of existing studies rely on synthetically generated datasets, primarily due to the low probability and random nature of real anomaly occurrences, which make it difficult to collect large-scale labeled real-world data. This limitation significantly hampers the empirical validation of detection algorithms. Even in the dataset introduced by Kim et al. [51] where real-world signals were captured, the anomalies themselves were synthetically injected into the data stream. Detailed of available datasets is provided in Table 6. As can be observed, the dataset introduced in [51] demonstrates remarkable scale and diversity, featuring IQ and spectrogram data across various LTE/5G bands, realistic Extended Typical Urban (ETU) fading conditions, and a variety of anomalies such as tone, chirp, and pulse. Notably, one of its unique features is the inclusion of wideband signals, emphasizing a focus on wideband scenarios. In contrast, other datasets such as those by Swinney et al. [54], Ujan et al. [46, 62], and Morales Ferre et al. [27]primarily focus on narrowband GNSS or DVB-S2 signals and feature fewer anomaly types, often limited to CWI, MCWI, or chirp jammers. The dataset introduced by Kulin et al.[18], while offering

broader frequency coverage and a larger sample volume, was not designed for localization tasks.

This comparison underscores the need for future datasets to incorporate a broader range of anomaly types, alongside both narrowband and wideband communication signals, in order to better reflect the complexity of real-world spectrum environments. Specifically, the ability to distinguish between narrowband anomalies and legitimate narrowband communications, and similarly between wideband anomalies and wideband communications, represents a fundamental challenge for spectrum monitoring and awareness systems. Addressing this challenge requires datasets that capture both types of signals in realistic and dynamic environments.

Future research can extend into the domain of wideband spectrum monitoring, where a variety of signals with differing bandwidths may coexist with spectral anomalies. In this context, segmentation-based and object detection methods can be explored to differentiate anomalies from legitimate signals and to localize them across a wideband range.

Another limitation of current research is the lack of attention to post-detection analysis of anomaly behavior. Understanding characteristics such as periodicity, persistence, recurrence patterns, and amplitude variations, can significantly contribute to a deeper understanding of anomaly nature, distinguishing between transient and persistent anomalies, and making more informed and effective decisions.

TABLE 5
Summary of Spectrum Anomaly Detection Studies Using Deep Learning

Reference	**Year**	**Approach**	**Model**	**Anomaly**	**Dataset Availability**
Feng et al. [50]	2017	Reconstruction	Deep Autoencoder	Unknown	✕Real
Kulin et al.[18]	2018	Classification	CNN with two convolutional layer, and two fully connected layer	Known	✓ Real[78]
Davaslioglu et al. [40]	2019	Classification	The features extracted from the denoising autoencoder are fed into the CNN and FNN	Known	✕Synthetic
Morales Ferre et al. [27]	2019	Classification	CNN with one convolutional layer, and one fully connected layer, and SVM	Known	✓Synthetic
Rajendran et al. [13]	2019	Reconstruction	Adversarial Autoencoders	Unknown	✕Synthetic
Toma et al. [58]	2020	Reconstruction	Conditional GAN, and Variational Autoencoder	Unknown	✕Real
Ujan et al.[62]	2020	Classification	Pretrained CNNs including AlexNet[65], GoogleNet[79], ResNet18[68], VGG16[67]	Known	✓ Real
Ujan et al. [46]	2020	Classification	Multilayer perceptron	Known	✓ Real
Zhou et al. [32]	2021	Reconstruction	Generative Adversarial Network	Unknown	✕ Synthetic
Bhatti et al. [19]	2021	Classification	VGG [67], ResNet[68]	Known	✕Real
Qin et al. [55]	2022	Object detection	Combined backbone-based CSPDarknet with Neck-based APNet	Known	✕ Synthetic
Xu et al. [41]	2022	Classification	CNN	Known	✕Real
Kuang et al.[65]	2022	Reconstruction	IMemAE	Unknown	✕ Synthetic
Peng et al. [45]	2022	Reconstruction and segmentation	Combining CNNs and LSTM networks	Known	✕ Synthetic
Huang et al. [29]	2023	Reconstruction	Masked Autoencoders	Unknown	✕Real
Swinney et al.[54]	2023	classification	VGG-16 for the feature extraction, k-means for classification	Known	✓ Synthetic
Zeng et al. [66]	2023	Reconstruction	AE-DDPMs	Unknown	✕ Synthetic
Liu et al. [28]	2023	Recognition	DenseNet[80]	Known	✕ Synthetic
Reda et al.[42]	2023	Classification	BiLSTM-Attention	Known	✓ Real
Qi, et al. [12]	2024	Reconstruction	Unsupervised Deep Memory Autoencoders	Unknown	✕ Synthetic
Jiang et al. [53]	2024	Classification	CNN, VGG16[67]	Known	✓Synthetic [27]
Steiner et al. [52]	2024	Classification	ResNet models	Known	✕Real
El-Haryqy et al. [63]	2024	Object detection	Mask R-CNN	Known	[62]
Liu et al. [49]	2024	Reconstruction	VAE with Adaptive Attention	Unknown	✕Real
Kim et al. [51]	2024	Object Detection	YOLOv11, RT-DETR, CenterNet	Known	✓ Real+Synthetic

TABLE 6
Comparison of Available Datasets for Deep Learning-Based Spectrum Anomaly Detection

Characteristics	**Kulin et al.[18]**	**Morales Ferre et al. [27]**	**Ujan et al. [46]**	**Ujan et al.[62]**	**Swinney et al. [54]**	**Kim et al. [51]**
Data Type	IQ, Amplitude/Phase, Frequency	Spectrogram Image	Scalogram image	Feature vector	Combined image views (Spectrogram, Histogram, etc.)	IQ Data, Spectrogram
Data Format	Vector (2×128), Time-Frequency	Grayscale (512×512)	RGB Image (224×224)	I/Q vector	Combined image (224×224)	IQ Vectors Spectrogram: RGB Image (400×400)
Number of Samples	225,225	61,800	4,800	4,800	~600	190,000
Anomaly Type	Technology interference (WiFi, BT, etc.)	AM, FM, Chirp, Pulse, Narrow Band	CWI, MCWI, Chirp	CWI, MCWI, Chirp	AM, FM, Chirp, Pulse, Narrow Band jamming	SingleTone, Chirp, Pulse
Frequency Band	ISM (2.4 GHz)	GNSS L1 (~1.5 GHz)	DVB-S2 (Satellite, 40 MHz sampling)	DVB-S2 (Satellite, 40 MHz sampling)	GNSS	19 LTE & 5G bands (862 MHz to 3712 MHz)
Conditions / Impairment	Random SNR, synthetic fading, channel models	SNR = 25–50 dB, JSR = 40–80 dB	SNR ≈ 9 dB, AWGN = –140 dBm, JSR = 5–8 dB	SNR ≈ 9dB, JSR = 5–8dB	AWGN, Fixed SNR, JSR=40–80 dB	ETU fading model, SNR= –10 to +10 dB, ISR= –10 to +10 dB

7. Conclusion

This paper provides a comprehensive review of the application of deep learning in spectrum anomaly detection, with an emphasis on pre-processing techniques and problem-solving strategies. The analysis highlights that pre-processing methods, such as spectrograms, despite their computational cost, offer valuable time-frequency information that is essential for effective anomaly detection. Furthermore, the study underscores the versatility of deep learning approaches, including classification, object detection, reconstruction, and segmentation, which can be tailored to specific application requirements. Building on these findings, the paper emphasizes the need for future research to address several critical areas. Enhancing the efficiency of pre-processing methods, such as Q-spectrogram, can further reduce computational demands while maintaining high-resolution outputs. Additionally, advancing deep learning models to better handle dynamic and low-SNR environments can improve their robustness in real-world scenarios.

Acknowledgment

No organization funded this research. M. Aghalari designed the model, implemented the research, and wrote the original version of the draft. H. Khaleghi Bizaki helped the main idea, validated the methodology and reviewed the final version.

References

[1] Y. Zhang & Z. Luo. (2023). A review of research on spectrum sensing based on deep learning. *Electronics*. [Online]. *12(21)*, p. 4514. Available: https://doi.org/10.3390/electronics12214514

[2] Y. Molina‑Tenorio, A. Prieto‑Guerrero, R. Aguilar‑Gonzalez, & S. Ruiz‑Boqué. (2019). Machine learning techniques applied to multiband spectrum sensing in cognitive radios. *Sensors*. [Online]. *19(21)*, p. 4715. Available: https://doi.org/10.3390/s19214715

[3] V. Chandola, A. Banerjee, & V. Kumar. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*. [Online]. *41(3)*, pp. 1–58. Available: https://doi.org/10.1145/1541880.1541882

[4] Z. Yang & R. J. Radke, “Context‑aware video anomaly detection in long‑term datasets,” In Proceeding IEEE/CVF Conference computer vision and pattern recognition (cvpr), 2024, pp. 4002–4011. Available: https://doi.org/10.1109/CVPR52733.2024.00372

[5] Y. Sreeraman, D. Jagadeesan, J. Jegan, T. Vivekanandan, A. Srinivasan, & G. Asha. (2024). Enhancing anomaly detection in pedestrian walkways using improved sparrow search algorithm with parallel features fusion model. *Fusion: Practice & Applications*. [Online]. *14(2)*, pp. 119–131. Available: https://doi.org/10.54216/FPA.140210

[6] S. N. Chary & V. Ganesan, "Detection of abnormal events using deep learning in pedestrian walkways," In *G. H. L. Gururaj, F. Flammini, S. Srividhya, M. L. Chayadevi, & S. Selvam (Eds.), Computer Science Engineering: Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems (ICCIIS 2024)*, Bengaluru, India: CRC Press, 2024, pp. 299–306.

[7] P. Bonte, S. K. Hashemi, H. Hellbruck, and F. Jondral, “Unsupervised anomaly detection for communication networks: an autoencoder approach,” in *Proceeding International Workshop IoT, Edge, and Mobile for Embedded Machine Learning*, Cham, Switzerland:

Springer, 2020, pp. 160–172. Available: https://doi.org/10.1007/978-3-030-66770-2_12

[8] B. Lindemann, B. Maschler, N. Sahlab, & M. Weyrich. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*. [Online]. *131*, p. 103498. Available: https://doi.org/10.1016/j.compind.2021.103498

[9] T.-Y. Kim & S.-B. Cho. (2018). Web traffic anomaly detection using C‐LSTM neural networks. *Expert Systems with Applications*. [Online]. *106*, pp. 66–76. Available: https://doi.org/10.1016/j.eswa.2018.04.004

[10] J. S. Mambou, “Classification framework for anomaly detection in medical images,” Ph.D. dissertation, Faculty of Informatics and Management, Univ. of Hradec Králové, Hradec Králové, Czech Republic, 2021. [Online]. Available: https://theses.cz/id/34y9tk

[11] C. Baur, B. Wiestler, M. Muehlau, C. Zimmer, N. Navab, & S. Albarqouni. (2021). Modeling healthy anatomy with artificial intelligence for unsupervised anomaly detection in brain MRI. *Radiology: Artificial Intelligence*. [Online]. *3(3)*, p. e190169. Available: https://doi.org/10.1148/ryai.2020190169

[12] P. Qi, T. Jiang, J. Xu, J. He, S. Zheng, & Z. Li. (2024). Unsupervised spectrum anomaly detection with distillation and memory‐enhanced autoencoders. *IEEE Internet of Things Journal*. [Online]. *11(24)*, pp. 39361–39374. Available: https://doi.org/10.1109/JIOT.2024.3424837

[13] S. Rajendran, W. Meert, V. Lenders, & S. Pollin. (2019). Unsupervised wireless spectrum anomaly detection with interpretable features. *IEEE Transactions on Cognitive Communications and Networking*. [Online]. *5(3)*, pp. 637–647. Available: https://doi.org/10.1109/TCCN.2019.2911524

[14] M. Khaleel, A. Jebrel, & D. M. Shwehdy. (2024). Artificial intelligence in computer science. *International Journal of Electrical Engineering and Sustainability*. [Online]. pp. 01–21. Available: https://doi.org/10.5281/zenodo.10937515

[15] Z. Zamanzadeh Darban, G. I. Webb, S. Pan, C. Aggarwal, & M. Salehi. (2024). Deep learning for time series anomaly detection: A survey. *ACM Computing Surveys*. [Online]. *57(1)*, pp. 1–42. Available: https://doi.org/10.1145/3625506

[16] D. Fährmann, L. Martín, L. Sánchez, & N. Damer. (2024). Anomaly detection in smart environments: A comprehensive survey. *IEEE Access*. [Online]. *12*, 64006–64049. Available: https://doi.org/10.1109/ACCESS.2024.3402107

[17] M. Rahmani & R. Ghazizadeh. (2022). Spectrum monitoring based on end‐to‐end learning by deep learning. *International Journal of Wireless Information Networks*. [Online]. *29(2)*, 180–192. Available: https://doi.org/10.1007/s10776-021-00530-4

[18] M. Kulin, T. Kazaz, I. Moerman, & E. De Poorter. (2018). End‐to‐end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications. *IEEE Access*. [Online]. *6*, 18484–18501. Available: https://doi.org/10.1109/ACCESS.2018.2818794

[19] F. A. Bhatti, M. J. Khan, A. Selim, & F. Paisana. (2021). Shared spectrum monitoring using deep learning. *IEEE Transactions on Cognitive Communications and Networking*. [Online]. *7(4)*, pp. 1171–1185. Available: https://doi.org/10.1109/TCCN.2021.3071149

[20] A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, and L. A. DaSilva, “Spectrum Monitoring for Radar Bands Using Deep Convolutional Neural Networks,” in Proceeding *2017 IEEE Global Communications Conference*, *GLOBECOM*, Singapore, 2017, pp. 1-6. https://doi.org/10.1109/GLOCOM.2017.8254105

[21] C. Hou, D. Fu, Z. Zhou, & X. Wu. (2023). A deep learning‐based multi‐signal radio spectrum monitoring method for UAV communication. *Drones*. [Online]. *7(8)*, p. 511. Available: https://doi.org/10.3390/drones7080511

[22] H. Pirayesh & H. Zeng. (2022). Jamming attacks and anti‐jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. [Online]. *24(2)*, pp. 767–809. 2022. Available: https://doi.org/10.1109/COMST.2022.3159185

[23] P. Lohan, B. Kantarci, M. A. Ferrag, N. Tihanyi, & Y. Shi. (2024). From 5G to 6G networks: A survey on AI‐based jamming and interference detection and mitigation. *IEEE Open Journal of the Communications Society*. [Online]. *5*, pp. 3920–3974. Available: https://doi.org/10.1109/OJCOMS.2024.3416808

[24] T. Oyedare, V. K. Shah, D. J. Jakubisin, & J. H. Reed. (2022). Interference suppression using deep learning: Current approaches and open challenges. *IEEE Access*. [Online]. *10*, pp. 66238–66266. Available: https://doi.org/10.1109/ACCESS.2022.3185124

[25] A. Lancho, J. Palacios, M. Selim, L. González, A. Krause, P. Casari, & X. Costa‐Pérez. (2025). RF Challenge: The data‐driven radio frequency signal separation challenge. *IEEE Open Journal of the Communications Society*. [Online]. *6*, pp. 4083–4100. Available: https://doi.org/10.22067/cke.2025.91456.1144

[26] X. Yang, A. Li, M. Wei, X. Zhang, S. Lu, and W. Wang, “Jamming Signal Detection Based on TSVD Method,” in *IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA)*, Dalian, China, 2020, pp. 558-562.

[27] R. Morales Ferre, A. De La Fuente, & E. S. Lohan. (2019). Jammer classification in GNSS bands via machine learning algorithms. *Sensors*. [Online]. *19(22)*, p. 4841. Available: https://doi.org/10.3390/s19224841

[28] M. Liu, Z. Liu, W. Lu, Y. Chen, X. Gao, & N. Zhao. (2021). Distributed few‐shot learning for intelligent recognition of communication jamming. *IEEE Journal of Selected Topics in Signal Processing*. [Online]. *16(3)*, pp. 395–405. Available: https://doi.org/10.1109/JSTSP.2021.3137028

[29] Y. Huang, S. Yuan, N. Liu, Q. Li, W. Liang, & L. Liu. (2023). Unsupervised interpolation recovery method for spectrum anomaly detection and localization. *Space: Science & Technology*. [Online]. *3*, p. 0082. Available: https://doi.org/10.34133/space.0082

[30] S. Hong, K. Kim, & S.-H. Lee. (2023). A hybrid jamming detection algorithm for wireless communications: Simultaneous classification of known attacks and detection of unknown attacks. *IEEE Communications Letters*. [Online]. *27(7)*, pp. 1769–1773. Available: https://doi.org/10.1109/LCOMM.2023.3275694

[31] M. Zhou, M. Kong, Y. Ye, B. Deng, & Y. Tang. (2024). Identifying sources of interference in civil aviation radio communication. *EURASIP Journal on Advances in Signal Processing*. [Online]. *(1)*, p. 88. Available: https://doi.org/10.1186/s13634-024-01185-5

[32] X. Zhou, J. Xiong, X. Zhang, X. Liu, & J. Wei. (2021). A radio anomaly detection algorithm based on modified generative adversarial network. *IEEE Wireless Communications Letters*. [Online]. *10(7)*, pp. 1552–1556. Available: https://doi.org/10.1109/LWC.2021.3079899

[33] K. Cohen & Q. Zhao. (2015). Active hypothesis testing for anomaly detection. *IEEE Transactions on Information Theory*. [Online]. *61(3)*, pp. 1432–1450. Available: https://doi.org/10.1109/TIT.2014.2371464

[34] M. Aghalari, A. Aghagolzadeh, & M. Ezoji. (2021). Brain tumor image segmentation via asymmetric/symmetric U‑Net based on two‑pathway‑residual blocks. *Biomedical Signal Processing and Control*. [Online]. *69*, p. 102841. https://doi.org/10.1016/j.bspc.2021.102841

[35] M. Aghalari & H. K. Bizaki. (2025). Enhancing of polyp image segmentation in colonoscopy images: A comprehensive approach using modified U‑Net, hybrid color space, and ensemble learning. *Multimedia Tools and Applications*. [Online]. *84(17)*, pp. 17491–17516. Available: https://doi.org/10.1007/s11042-024-19703-w

[36] M. U. Muzaffar & R. Sharqi. (2024). A review of spectrum sensing in modern cognitive radio networks. *Telecommunication Systems*. [Online]. *85(2)*, pp.347–363. Available: https://doi.org/10.1007/s11235-023-01079-1

[37] S. Peng, S. Sun, & Y.-D. Yao. (2021). A survey of modulation classification using deep learning: Signal representation and data preprocessing. *IEEE Transactions on Neural Networks and Learning Systems*. [Online]. *33(12)*, 7020–7038. Available: https://doi.org/10.1109/TNNLS.2021.3085433

[38] O. V. Ribeiro‑Filho, M. A. Ponti, M. Curilem, & R. A. Rios. (2025). Integrating wavelet transformation for end‑to‑end direct signal classification. *Digital Signal Processing*. [Online]. *156*, p. 104878. Available: https://doi.org/10.1016/j.dsp.2024.104878

[39] F. R. Guimarães, J. M. B. da Silva, Jr., C. C. Cavalcante, G. Fodor, M. Bengtsson, & C. Fischione. (2024). Machine learning for spectrum sharing: A survey. *Foundations and Trends in Networking*. [Online]. *14(1–2)*, pp. 1–159. Available: https://doi.org/10.1561/1300000073

[40] K. Davaslioglu, S. Soltani, T. Erpek, & Y. E. Sagduyu. (2021). DeepWiFi: Cognitive WiFi with deep learning. *IEEE Transactions on Mobile Computing*. [Online]. *20(2)*, pp. 429–444. Available: https://doi.org/10.1109/TMC.2019.2949815

[41] H. Xu et al. (2022). A neural network approach for wireless spectrum anomaly detection in 5G‑unlicensed network. *CCF Transactions on Pervasive Computing and Interaction*. [Online]. *4(4)*, pp. 465–473. Available: https://doi.org/10.1007/s42486-021-00075-1

[42] A. Reda, T. Mekkawy, T. A. Tsiftsis, & A. Mahran. (2024). Deep learning approach for GNSS jamming detection based on PCA and Bayesian optimization feature selection algorithm. *IEEE Transactions on Aerospace and Electronic Systems*. [Online]. *60(6)*, pp. 8349–8363. Available: https://doi.org/10.1109/TAES.2024.3429049

[43] C. Natalino, A. Udalcovs, L. Wosinska, O. Ozolins, & M. Furdek. (2021). Spectrum anomaly detection for optical network monitoring using deep unsupervised learning. *IEEE Communications Letters*. [Online]. *25(5)*, pp. 1583–1586. Available: https://doi.org/10.1109/LCOMM.2021.3055064

[44] S. Peng, H. Jiang, H. Wang, H. Alwageed, and Y.-D. Yao, "Modulation Classification Using Convolutional Neural Network Based Deep Learning Model," in *26th Wireless and Optical Communication Conference (WOCC)*, Newark, NJ, USA, 2017, pp. 1-5. Available: https://doi.org/10.1109/WOCC.2017.7929000

[45] C. Peng, W. Hu, & L. Wang. (2022). Spectrum anomaly detection based on spatio‑temporal network prediction. *Electronics*. [Online]. *11(11)*, p. 1770. Available: https://doi.org/10.3390/electronics11111770

[46] S. Ujan, N. Navidi, & R. Landry, Jr. (2020). An efficient radio frequency interference (RFI) recognition and characterization using end‑to‑end transfer learning. *Applied Sciences*. [Online]. *10(19)*, p. 6885. Available: https://doi.org/10.3390/app10196885

[47] N. Manakitsa, G. S. Maraslidis, L. Moysis, & G. F. Fragulis. (2024). A review of machine learning and deep learning for object detection, semantic segmentation, and human action recognition in machine and robotic vision. *Technologies*. [Online]. *12(2)*, p. 15p. Available: https://doi.org/10.3390/technologies12020015

[48] K. Tekbıyık, Ö. Akbunar, A. R. Ekti, A. Görçin, G. K. Kurt, & K. A. Qaraqe. (2021). Spectrum sensing and signal identification with deep learning based on spectral correlation function. *IEEE Transactions on Vehicular Technology*. [Online]. *70(10)*, pp. 10514–10527. Available: https://doi.org/10.1109/TVT.2021.3108184

[49] R. Liu, Q. Zhang, Y. Zhang, and C. Ma, "An Improved Wireless Spectrum Anomaly Detection Model with Adaptive Attention Mechanism," in Proc. *2024 8th International Conference on Control Engineering and Artificial Intelligenc*, Shanghai, China, 2024, pp. 79-84. Available: https://doi.org/10.1145/3640824.3640836

[50] Q. Feng, Y. Zhang, C. Li, Z. Dou, & J. Wang. (2017). Anomaly detection of spectrum in wireless communication via deep auto‑encoders. *The Journal of Supercomputing*. [Online]. *73(7)*, pp. 3161–3178. https://doi.org/10.1007/s11227-017-2017-7

[51] J. Kim, H. Kim, B. Kim, & S. Choi. (2024). Wireless anomaly signal dataset (WASD): An open dataset for

wireless cellular spectrum monitoring and anomaly detection. *IEEE Access*. [Online]. *12*, pp. 196240–196248. Available: https://doi.org/10.1109/ACCESS.2024.3521946

[52] J. Steiner & J. Pešík. (2024). Machine learning image recognition for GNSS jamming signals categorization. *Neural Network World*. [Online]. *34(6)*, pp. 341–360.

[53] M. Jiang, Z. Ye, Y. Xiao, and X. Gou, "Federated Transfer Learning Aided Interference Classification in GNSS Signals," in IEEE/CIC International Conference on Communications *China (ICCC)*, Hangzhou, China, Aug. 2024, pp. 1988-1993. Available: https://doi.org/10.1109/ICCC62479.2024.10681801

[54] C. J. Swinney and J. C. Woods, "GNSS Jamming Clustering Using Unsupervised Learning and Radio Frequency Signals," in Proceeding *International Conference Cybersecurity, Situational Awareness Social Media (ICCSSA), Cyber Science*, C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, and M. G. Jaatun, Eds. Copenhagen, Denmark: Springer, 2023, pp. 25-34. Available: https://doi.org/10.1007/978-981-99-6974-6_2

[55] J. Qin, F. Zhang, K. Wang, Y. Zuo, & C. Deng. (2022). Interference signal feature extraction and pattern classification algorithm based on deep learning. *Electronics*. [Online]. *11(14)*, p. 2251. Available: https://doi.org/10.3390/electronics11142251

[56] O. Özhan. (2022). Short‑time Fourier transform. In *Basic Transforms for Electrical Engineering*. Cham, Switzerland: Springer, 2022, pp. 441–464. Available: https://doi.org/10.1007/978-3-030-98846-3_7

[57] National Instruments, "STFT Spectrograms VI," *LabVIEW API Ref.*, 2024. [Online]. Available: https://www.ni.com/docs/en-US/bundle/labview-api-ref/page/vi-lib/gmath/trans-llb/stft-spectrograms-vi.html

[58] A. Toma, A. Krayani, L. Marcenaro, Y. Gao, and C. S. Regazzoni, "Deep Learning for Spectrum Anomaly Detection in Cognitive mmWave Radios," in *IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, London, U.K., 2020, pp. 1-7. Available: https://doi.org/10.1109/PIMRC48278.2020.9217240

[59] M. Chitgarha, A. Bozorgchenani, & M. J. Dehghani. (2017). On time compression overlap‑add technique in linear frequency modulation pulse compression radar systems: Design and performance evaluation. *IEEE Access*. [Online]. *5*, pp. 27525–27537. Available: https://doi.org/10.1109/ACCESS.2017.2771799

[60] M. Priyadarshini, M. Bajaj, L. Prokop, & M. Berhanu. (2024). Perception of power quality disturbances using Fourier, short‑time Fourier, continuous and discrete wavelet transforms. *Scientific Reports*. [Online]. *14(1)*, p. 3443. Available: https://doi.org/10.1038/s41598-024-53792-9

[61] P. N. Portela, "Improving speech prosody assessment through artificial intelligence," M.S. thesis, Fac. Eng., Univ. of Porto, Porto, Portugal, Oct. 2024.

[62] S. Ujan, N. Navidi, & R. Landry, Jr. (2020). Hierarchical classification method for radio frequency interference recognition and characterization in Satcom. *Applied Sciences*. [Online]. *10(13)*, p. 4608. Available: https://doi.org/10.3390/app10134608

[63] N. El‑haryqy, Z. Madini, & Y. Zouine. (2024). Radio frequency interference detection and automatic modulation recognition based on Mask RCNN. *International Journal of Computer Networks and Communications*. [Online]. *16(5)*, pp. 23–42.

[64] J. Y. Chen & B. Z. Li. (2024). The short‑time Wigner–Ville distribution. *Signal Processing*. [Online]. *219*, p. 109402. Available: https://doi.org/10.1016/j.sigpro.2024.109402

[65] T. Kuang, B. Zhou, J. Li, G. Ding, & Q. Wu. (2022). Abnormal communication signals recognition based on image enhancement and improved memory‑augmented autoencoder. *Wireless Communications and Mobile Computing*. [Online]. *2022*, p. 7228511. Available: https://doi.org/10.1155/2022/7228511

[66] J. Zeng, X. Liu, & Z. Li. (2023). Radio anomaly detection based on improved denoising diffusion probabilistic models. *IEEE Communications Letters*. [Online]. *27(8)*, pp. 1979–1983. Available: https://doi.org/10.1109/LCOMM.2023.3290813

[67] K. Simonyan & A. Zisserman. (2014). Very deep convolutional networks for large‑scale image recognition. *arXiv preprint arXiv:1409.1556*. [Online]. Available: https://arxiv.org/abs/1409.1556

[68] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in *IEEE conference on computer vision and pattern recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 770-778.

[69] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, & K. Keutzer. (2016). SqueezeNet: AlexNet‑level accuracy with 50× fewer parameters and <0.5 MB model size. *arXiv preprint arXiv:1602.07360*. [Online]. Available: https://arxiv.org/abs/1602.07360

[70] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation," in *Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR)*, Columbus, OH, USA, 2014, pp. 580-587.

[71] R. Girshick. (2015). Fast R‑CNN. *arXiv preprint arXiv:1504.08083*. [Online]. Available: https://arxiv.org/abs/1504.08083

[72] S. Ren, K. He, R. Girshick, & J. Sun. (2017). Faster R‑CNN: Towards real‑time object detection with region proposal networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. [Online]. *39(6)*, pp. 1130–1144. Available: https://doi.org/10.1109/TPAMI.2016.2577031

[73] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, Las Vegas, NV, USA, 2016, pp. 779-788.

[74] C. Liu, Y. Tao, J. Liang, K. Li, and Y. Chen, "Object Detection Based on YOLO Network," in *IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, Chongqing, China, 2018, pp. 799-803. https://doi.org/10.1109/ITOEC.2018.8740604

[75] T. Diwan, G. Anirudh, & J. V. Tembhurne. (2023). Object detection using YOLO: Challenges,

architectural successors, datasets and applications. *Multimedia Tools and Applications*. [Online]. *82(6)*, 9243–9275. Available: https://doi.org/10.1007/s11042-022-13644-y

[76] C. I. Bercea, D. Rueckert, and J. A. Schnabel, "What Do AEs Learn? Challenging Common Assumptions in Unsupervised Anomaly Detection," in Proc. *Int. Medical Image Computing and Computer Assisted Intervention (MICCAI), Vancouver*, BC, Canada, 2023, pp. 304-314. Available: https://doi.org/10.1007/978-3-031-43904-9_30

[77] K. Berahmand, F. Daneshfar, E. S. Salehi, Y. Li, & Y. Xu. (2024). Autoencoders and their applications in machine learning: A survey. *Artificial Intelligence Review*. [Online]. *57(2)*, p. 28. Available: https://doi.org/10.1007/s10462-023-10692-0

[78] M. Schmidt, D. Block, and U. Meier, "Wireless Interference Identification With Convolutional Neural Networks," in *IEEE 15th IEEE 15th International Conference on Industrial Informatics (INDIN)*, Emden, Germany, 2017, pp. 180-185. Available: https://doi.org/10.1109/INDIN.2017.8104767

[79] C. Szegedy *et al.*, "Going deeper with convolutions," in Proceeding *IEEE conference on computer vision and pattern recognition (CVPR)*, 2015, pp. 1-9.

[80] Y. Zhu and S. Newsam, "Densenet for dense flow," *in IEEE international conference on image processing (ICIP)*, 2017, pp. 790-794. Available: https://doi.org/10.1109/ICIP.2017.8296389